Department of Health and Human Services

DEPARTMENTAL APPEALS BOARD

Civil Remedies Division

Director of the Office for Civil Rights

v.

The University of Texas MD Anderson Cancer Center.

Docket No. C-17-854

Decision No. CR5111

Date: June 1, 2018

DECISION

I grant summary judgment in favor of the United States Department of Health and Human Services, Office for Civil Rights (OCR) and against Respondent, The University of Texas MD Anderson Cancer Center. I sustain imposition of the following remedies against Respondent:

- To remedy Respondent's noncompliance with 45 C.F.R. § 164.312(a), civil money penalties of $2,000 per day for each day of a period that began on March 24, 2011 and that continued through January 25, 2013; and

- To remedy Respondent's noncompliance with 45 C.F.R. § 164.502(a), civil money penalties of $1,500,000 per year for the years 2012 and 2013.

The daily civil money penalties that I impose remedy Respondent's failure to encrypt electronic devices including laptop computers and USB thumb drives pursuant to the requirements of law. The annual civil money penalties that I impose remedy Respondent's unlawful disclosure of electronic Protected Health Information ("ePHI") relating to about 30,000 individuals in 2012 and more than 3500 individuals in 2013.[1] The term "ePHI" encompasses electronically stored

[1] These numbers are approximate but they are not disputed. It is unnecessary that I make findings as to the exact number of individuals whose ePHI Respondent unlawfully disclosed.

protected information about patients consisting of: identifying information such as patient names, addresses, and Social Security numbers; and clinical information such as diagnoses, assessments, prognoses, and treatment regimes.

I. Background

OCR moved for summary judgment against Respondent and Respondent cross-moved for summary judgment. With its motion OCR filed 85 proposed exhibits that it identified as OCR Ex. 1-OCR Ex. 85. In opposing the motion and cross-moving Respondent filed 80 proposed exhibits that it identified as R. Ex. 1-R. Ex. 80. OCR filed a brief and a reply brief in support of its motion. Respondent filed a brief in opposition to OCR's motion and a sur-reply brief. In referring to the parties' briefs in this decision I refer to "OCR brief," "OCR reply," "Respondent brief," and "Respondent sur-reply."

I do not receive the parties' proposed exhibits into evidence. It is unnecessary inasmuch as I base this decision solely on undisputed material facts. I refer to some of the exhibits but only to illustrate facts that are not disputed.

II. Issues, Findings of Fact and Conclusions of Law

A. Issues

This case concerns Respondent's alleged failure to comply with regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA). 42 U.S.C. § 1320d-5; 45 C.F.R. Part 160, Subpart D and 45 C.F.R. Part 164, Subparts A, C, D, and E. Essentially, OCR alleges that Respondent failed to comply with regulatory requirements in two respects: (1) it failed to perform its self-imposed duty to encrypt electronic devices and data storage equipment; and (2) it allowed ePHI to be disclosed. The issues raised by OCR's allegations are whether:

1. Respondent failed to comply with HIPAA regulatory requirements; and
2. OCR's determinations to impose civil money penalties against Respondent are reasonable.

Respondent opposes OCR's assertions and its determinations of regulatory violations. It denies that it was obligated to encrypt its devices. It asserts that it did not contravene regulatory requirements governing disclosure of ePHI. It contends that the ePHI at issue is "research" and is not subject to HIPAA non-disclosure requirements. It argues that the penalties that CMS determined to impose against it are unreasonable and contrary to that which is permitted by regulation. I address these arguments in this decision.

Respondent makes three additional arguments that I do not address. First, it contends that as an agency of Texas' state government its activities lie beyond the reach of HIPAA. It argues that it is not a "person" as is defined by HIPAA. Respondent brief at 21-26. Respondent concedes that it is a "person" within the meaning of the regulatory definition of that term at 45 C.F.R. § 160.103. Respondent asserts that the regulation's definition of a "person" exceeds the statutory definition of that term.

Effectively, Respondent's argument is that the regulations published by the Secretary of the United States Department of Health and Human Services ("Secretary") are *ultra vires* HIPAA because they unlawfully broaden the statute's definition of "person" to include an agency of a state government. I have no authority to address this argument. My authority to hear and decide this case rests entirely on a delegation from the Secretary. Nothing in that delegation authorizes me to find that the Secretary's regulations are *ultra vires*. *See* 45 C.F.R. § 160.508. Consequently, I must apply those regulations to the facts of this case.

Second, Respondent argues that OCR ignored statutory caps on civil money penalties in determining the penalties that it requests that I impose. Respondent brief at 50-53. It contends that HIPAA, as amended, allows at most, penalties of $100,000 per year, and it contends that regulations that allow higher penalties than this asserted $100,000 annual ceiling constitute a misinterpretation of the statute. *See* 45 C.F.R. § 160.404.

This argument is a second attempt by Respondent to have me declare regulations to be *ultra vires*. I have no authority to consider this argument for the reasons that I have explained. Respondent argues, however, that I have the authority to reduce civil money penalties, citing 45 C.F.R. § 160.546(b). It asserts that I should reduce the proposed penalties to amounts at or below the asserted statutory cap because doing so would adhere to statutory limitations. I may not do that, first, because to do so would constitute an end run around the Secretary's intent as expressed in the regulations and second, because in evaluating civil money penalty amounts I must limit my review to the aggravating and mitigating factors set forth at 45 C.F.R. § 160.408.

Third, Respondent asserts that the civil money penalties proposed by OCR violate the excessive fines provision of the Eighth Amendment of the United States Constitution, and it asks me to declare those proposed penalties to be arbitrary and unconstitutional. Respondent brief at 58-62. I do not address this argument because my delegated authority does not include the authority to declare unconstitutional proposed actions by agencies of this Department.

Respondent, professing to recognize the limits of my authority, asserts that I should apply the principles embodied in the Eighth Amendment to the facts of this case even if I do not declare the proposed penalties to be unconstitutional. That is yet another effort by Respondent to have me exceed my limited authority. I decide the reasonableness of the penalty amounts strictly based on the criteria set forth in the applicable regulations.

B. Findings of Fact and Conclusions of Law

1. Respondent's Noncompliance with Regulatory Requirements

The Secretary published regulations that implement those sections of HIPAA that require him to promulgate standards for the electronic exchange, privacy, and security of health information. These regulations are set forth at 45 C.F.R. pt. 160 and 45 C.F.R. pt. 164, subpts. A, C, D, and E. In general entities that are covered by these regulations are required to: ensure the confidentiality, integrity, and availability of all ePHI that the entities create, receive, maintain, or transmit; protect such information against any reasonably anticipated threats or hazards to its security; protect ePHI against any reasonably anticipated impermissible uses and disclosures; and ensure compliance with these requirements by their workforces. 45 C.F.R. § 164.306(a).

Additional regulations implement these requirements. OCR alleges that Respondent failed to comply with certain of these implementing regulations.

OCR alleges that Respondent failed to comply with the requirements of 45 C.F.R. § 164.312. OCR brief at 25-26. This regulation requires, at subsection (a)(1), that an entity covered by HIPAA must implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access. Put more simply, the subsection requires a health care provider to protect its electronic information systems from disclosure of ePHI to unauthorized individuals or data systems.[2] At subsection (a)(2), the regulation requires a covered entity to implement, among other things, a mechanism to encrypt and decrypt ePHI.

OCR asserts that Respondent violated these regulatory requirements because it failed to assure encryption of laptop computers and USB drives that contained ePHI generated or maintained by Petitioner or its staff.

---

[2] The term "covered entity" is defined at 45 C.F.R. § 160.103 to include a health care provider that transmits any health information in electronic form in connection with a covered transaction. The same section defines a "transaction" to include a wide variety of information transmissions.

OCR alleges additionally that Respondent failed to comply with the requirements of 45 C.F.R. § 164.502(a). OCR brief at 26. Subsection (a) of this regulation prohibits a covered entity from using or disclosing ePHI except as is specifically permitted elsewhere in the regulation. OCR contends that Respondent violated this regulation when an unencrypted laptop computer containing ePHI was stolen and when its agents or its employees lost unencrypted USB flash drives containing unencrypted ePHI. OCR argues that the loss of ePHI constitutes an unlawful disclosure of that information, relying on the definition of disclosure at 45 C.F.R. § 160.103. That section defines the term to include any "release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information." *Id.* In advancing this argument OCR acknowledges that a covered entity is not required to guarantee the safety of ePHI. However, according to OCR, it must reasonably safeguard protected information from unlawful disclosure. 45 C.F.R. § 164.530(c)(2)(i).

The undisputed material facts establish that Petitioner failed to comply with these regulations. These facts establish that Petitioner, a comprehensive cancer center that operates both inpatient and outpatient facilities in the Houston, Texas area, was not only aware of the need to encrypt devices in order to assure that confidential data including ePHI not be improperly disclosed, but it established a policy requiring the encryption and protection of devices containing ePHI. However, and despite this awareness and its own policies, Petitioner made only half-hearted and incomplete efforts at encryption over the ensuing years. As a consequence, the theft of a laptop computer that was not encrypted and the loss of two unencrypted USB thumb drives resulted in the unlawful disclosure of ePHI relating to tens of thousands of Respondent's patients.

Respondent recognized the need to encrypt data as early as 2006. Then, and subsequently, it consistently stated that confidential data, including ePHI, must be protected against loss or theft, and it repeatedly announced a policy that both required encryption of confidential data and prohibited unsecured storage of such data. Respondent's 2006 version of its Information Resources Security Operations Manual ("manual") and subsequent versions set forth procedures and policies governing its implementation of HIPAA requirements. OCR Ex. 1 at 3. The 2006 edition of the manual explicitly requires that data stored on media, including transportable media and laptops, that travel from Respondent's premises must be encrypted or protected with access controls. *Id.* at 24. The manual enjoins Respondent's employees from unauthorized removal of devices containing confidential data, and it directs that such data stored on transportable media must be encrypted. *Id.* at 25, 29. The 2006 version additionally states that devices containing confidential information must not be left unattended and must be physically secured at all times. *Id.* at 29.

Respondent or Respondent's parent, the University of Texas System, stated these policies in additional documents. In 2007, the University of Texas System advised its subsidiaries and affiliates that many incidents involving unauthorized exposure of confidential data result from theft or loss of portable devices that contain such data. OCR Ex. 2 at 2. It directed that as a general principle, confidential data should not be stored on portable devices or on privately-owned devices. It added, however, that any confidential data that is stored on such devices must be encrypted using approved methods. *Id.* In November 2007, Respondent issued a confidentiality policy and a patient privacy policy stating that appropriate safeguards must be taken to protect the confidentiality of patients' health information. OCR Ex. 3; OCR Ex. 4.

Respondent often reiterated its policies concerning protection and non-disclosure of confidential information including ePHI. For example, in 2011 it restated its prohibition against the unauthorized removal by employees from its premises of confidential information. OCR Ex. 7 at 69.

The policies enunciated by Respondent and its parent are consistent with the risk of unauthorized disclosure of confidential information including ePHI that Respondent identified and assessed. In 2007 Respondent identified mobile media security as a high level risk. OCR Ex. 26 at 4-5.

Respondent eventually determined that the mechanism with which it would protect confidential data including ePHI would be the encryption of the devices on which such data is stored. In 2008 Respondent announced that it intended to implement the first phase of a media security project that would test and implement encryption of institutional laptop and desktop computers. OCR Ex. 9 at 10.

However, despite identifying the risk of and dangers related to confidential data loss and deciding on encryption of devices as a means of protecting such data, Respondent delayed encryption of laptop devices for years and then, proceeded with encryption at a snail's pace. In 2009, for example, Respondent declared that it was putting laptop encryption efforts on hold due to financial constraints. OCR Ex. 10 at 6; OCR Ex. 27 at 1, 4. As of then, it had not encrypted any of the several thousand laptops that it controlled. OCR Ex. 27 at 4. In 2010, citing the theft of a laptop and other instances of lost records, Respondent's director of information security proposed restarting efforts to encrypt laptops. OCR Ex. 28 at 1. However, as of August 2011, Respondent had not commenced laptop encryption, three years after it announced that it would encrypt its computers, and despite its continued recognition that lack of encryption put its confidential data at high risk. OCR Ex. 11 at 11, 13, 15; OCR Ex. 14.

There are no facts to suggest that Respondent developed alternate means to protect confidential information during the years when it delayed encrypting mobile storage devices. Respondent's self-selected method for confidential data protection – encryption of devices – constituted its primary protective mechanism, but Respondent failed to activate that mechanism.

Respondent did not finally begin mass encryption of its laptops until May 2012. OCR Ex. 39 at 5. The University of Texas System set a goal of August 31, 2012, for encryption of all university laptop computers. OCR Ex. 41. However, as of November 2013, Respondent had not fully encrypted its computers. As of that date more than ten percent of its computers remained unencrypted. OCR Ex. 71 at 3. More than 4400 computers were not encrypted as of that date. *Id.* As of January 2014 nearly ten percent of Respondent's computers – more than 2600 devices – remained unencrypted. *Id.* at 4.

Respondent plainly recognized that its halting efforts at encryption of computers created a high risk of unauthorized disclosure of confidential information including ePHI. For example, in June 2013, Respondent's institutional compliance officer issued an annual risk analysis that identified failure to encrypt data as a high risk impact area. OCR Ex. 22 at 2. The analysis identified a high degree of risk from: "[f]ailure to prevent unauthorized downloading of ePHI, [c]onfidential and [r]estricted [c]onfidential [i]nformation on to portable computing devices." *Id.*

Respondent understood that the need to protect confidential information including ePHI required more than just encrypting laptops and other computers. There also was a risk of unauthorized disclosure resulting from the loss of data storage devices. However, Respondent did not purchase and distribute encrypted USB devices ("IronKeys") until September 2012 after the loss of an unencrypted USB device. OCR Ex. 47; OCR Ex. 48.

On April 30, 2012, someone stole a laptop computer from the home of one of Petitioner's employees, an individual employed as a clinician, a clinical researcher, and Director of Research Informatics at Respondent's Genitourinary Center. OCR Ex. 55 at 1; OCR Ex. 56; OCR Ex. 57 at 2; OCR brief at 22. That employee had purchased the computer with Respondent's funds. He used it as a telework computer. OCR Ex. 57 at 2; OCR Ex. 59. The computer was neither encrypted nor was it password protected. *Id.* It contained ePHI relating to almost 30,000 individuals. OCR Ex. 57 at 2; OCR Ex. 58. The ePHI stored on the laptop included patients' names, Social Security numbers, medical record numbers, and treatment and/or research information. OCR Ex. 56.

On July 13, 2012, one of Respondent's employees (a trainee) lost a USB thumb drive belonging to Respondent while riding on one of Respondent's employee shuttle buses. The drive was not encrypted and it contained ePHI relating to more than 2200 individuals. OCR Ex. 63. The trainee had been authorized on multiple occasions by her supervisor to take the drive home. OCR Ex. 64 at 2-3. The ePHI on the lost thumb drive included patients': names; dates of birth; medical record numbers and diagnoses; and treatment and research information. OCR Ex. 63. An internal review conducted by Respondent concluded that Respondent's staff violated information disclosure policies by allowing the employee to transport ePHI away from the workplace on an unencrypted thumb drive. OCR Ex. 60 at 2.

On or after November 27, 2013, a visiting researcher at Petitioner's facility lost an unencrypted USB thumb drive containing ePHI relating to about 3600 individuals. OCR Ex. 73 at 2. The missing thumb drive likely contained patient information including patients': names; dates of birth (in a few instances); medical record numbers; diagnoses; and treatment and research information. *Id.*

I find Respondent's defenses to be without merit.

Respondent contends that it was not required by regulation to encrypt its devices. Relying on the text of 45 C.F.R. § 164.312(a)(2)(iv), Respondent contends that it was required only to "implement a mechanism to encrypt and decrypt electronic protected health information." The requirement that it implement a mechanism, according to Respondent, excluded any requirement that it actually encrypt devices. Respondent brief at 26-35. Respondent goes on to argue that it adopted and implemented a "mechanism" that included the following features:

- Password protection of all computers and portable computing devices accessing potentially confidential information;

- A requirement that confidential or protected data stored on portable computing devices must be encrypted and backed up to a network server in the event of a disaster or loss of information;

- Annual employee training event that provided its employees with training in areas that included ePHI transmission and proper disposal; a prohibition against password sharing; a discussion of password necessity and integrity; an explanation of authorized and proper use of information systems, and training about information security resources.

Respondent brief at 29-30. Respondent concludes by characterizing encryption of devices as optional, but asserts that it made substantial efforts to accomplish that.

This argument is a red herring. The regulations governing ePHI do not specifically require devices to be encrypted if "encryption" in this context is interpreted to mean some mechanical feature that renders these devices physically impossible to enter by any persons who are not authorized users. But, these regulations require covered entities to assure that all systems containing ePHI be inaccessible to unauthorized users. 45 C.F.R. § 164.306(a); 45 C.F.R. § 164.312(a)(1).

These regulations give considerable flexibility to covered entities as to how they protect their ePHI. Nothing in those regulations directs the use of specific devices or specific mechanisms by a covered entity. However, the bottom line is that whatever mechanisms an entity adopts must be effective.

Respondent failed to comply with regulatory requirements because it failed to adopt an effective mechanism to protect its ePHI. As early as 2006 Respondent recognized its vulnerability to loss of confidential information including ePHI. In 2008 Respondent decided that it would encrypt its devices, including laptops and USB drives, in order to protect any ePHI that these devices contained. Encryption of devices wasn't a mechanism specifically dictated by the regulations. But, it was the mechanism that Respondent chose to protect its ePHI contained on portable devices. Once Respondent elected to utilize that mechanism, it was obligated to make it work.

Manifestly, Respondent failed to do so. It delayed for years implementing its self-selected mechanism for protecting ePHI, encryption of portable devices. In 2013 Respondent had still not encrypted all of its devices. That was five years after Respondent chose to encrypt its devices as a data protection mechanism.

The approaches touted by Respondent were not intended to substitute for encryption. Respondent has pointed to no facts that suggest or establish that at some point after 2008 it decided to implement alternate mechanisms other than encryption to protect its ePHI. However, even if Respondent adopted the various approaches in lieu of encrypting devices that it asserts were its mechanism to protect ePHI, those approaches failed spectacularly to protect Respondent's confidential data, with ePHI pertaining to more than 33,000 individuals being lost or stolen in 2012 and 2013.

Next, Respondent asserts that it did not commit an unlawful disclosure of ePHI in violation of 45 C.F.R. § 164.502(a). It divides this argument into three subparts.

First, it contends that the loss of confidential information including ePHI resulting from the stolen laptop and lost thumb drives wasn't a "disclosure" as is defined by regulation. Respondent brief at 37-43. Respondent points to regulatory language

defining "disclosure" to be the "release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information." 45 C.F.R. § 160.103. It argues that a critical element of this definition is that, in order to be disclosed, any lost confidential information that is lost by an entity must be received or viewed by someone outside of the entity. Respondent brief at 37. Respondent contends that the undisputed facts of this case fail to show that any of the lost information was received or viewed by anyone.

I find nothing in the regulation that suggests that lost information must be viewed by unauthorized individuals in order to be disclosed. The plain language of the regulation doesn't suggest that. Moreover, to interpret the regulation so narrowly as Respondent suggests would render its prohibitions against unauthorized disclosure to be meaningless. If Respondent had its way, it and other covered entities could literally cast ePHI to the winds and be immune from penalty so long as OCR fails to prove that someone else received and viewed that information.

The regulation defines disclosure as including "release" of confidential information. The word "release" has a common and ordinary meaning. "Release" means to set free from restraint, confinement, or servitude. https://www.merriam-webster.com/dictionary/release. It is the act of setting something free that constitutes a "release," not a third party recapturing that which has been released. Thus, the regulation makes it plain that any loss of ePHI is a "release," and consequently, a disclosure of that information.

Respondent attempts to support its cramped definitions of "release" and "disclosure" by relying on two decisions involving alleged breaches of the Privacy Act, a federal statute that gives individuals a remedy against unlawful disclosure of certain confidential information. Respondent cites *Luster v. Vilsack,* 667 F.3d 1089, 1097-98 (10th Cir. 2011), and *In re Science Applications Int'l Corp. Backup Tape Data Theft Litig.*, 45 F.Supp. 3d 14, 28 (D.D.C. 2014). According to Respondent both of these cases stand for the principle that no cause of action for unlawful disclosure of confidential information may exist absent proof that an unauthorized individual or entity actually received the information.

These cases clearly are distinguishable from this case. Both cases involved private claims for damages based on alleged unlawful disclosures of confidential information. The courts in both cases reasoned that no private right of action could exist absent proof of some damages and such damages could result only from receipt of disclosed confidential information. This case does not involve a private suit for damages. It addresses the authority of an agency of government to remedy the unauthorized release of ePHI by covered entities. The statutory authority to impose a remedy hinges on the *release* and not the *receipt* of such

information, because under HIPAA the Secretary is obligated to protect ePHI and not just simply redress the consequences of unlawful disclosure.

The purpose of HIPAA and its implementing regulations explicitly is to protect against failures and omissions by covered entities that might result in such consequences as identity theft or other invasions of privacy. If Respondent had its way, HIPAA would become unenforceable in most instances. How could anyone know with any reasonable probability that – for example – the ePHI contained on the stolen laptop resulted in a given individual suffering from identity theft? It would be impossible in most instances to ascertain whether that is so.

Second, Respondent asserts that HIPAA doesn't apply in this case because the ePHI contained in the stolen and lost devices was research information that is outside of the statute and regulations' reach. Respondent brief at 43-44. This argument rests on what is at best a fanciful interpretation of governing regulations, and I find it to be without merit.

Respondent predicates this argument on its assertion that an exemption applies to all information or data that is used in research. Under Respondent's formulation, even patient data that reveals the names of patients, their social security numbers, their medical diagnoses, and the treatments that they are receiving is exempt from HIPAA requirements if used by someone in the course of research.

Respondent has identified nothing in the regulations that even ostensibly supports that argument. It contends, however, that the preamble to the regulations governing unauthorized disclosure makes it plain that the regulations do not apply to research information as Respondent defines that term. It cites to language in the regulations' preamble: "[W]e cannot apply any restrictions or requirements on a researcher in that person's role as a researcher . . . In its role as researcher, the person is not covered, and protections do not apply to those research records." Respondent brief at 43 (citing 65 Fed. Reg. 82,462, 82,575 (Dec. 28, 2000)). But, and as OCR notes, this language was meant to apply to the very limited instance of research conducted by non-covered entities and business associates that receive information from covered entities. OCR reply at 10-11.

Respondent's argument also ignores the fact that there is a regulatory mechanism for a facility to segregate its research function from its clinical function and to exempt its research function from non-disclosure requirements. 45 C.F.R. § 164.105; 65 Fed. Reg. 82,462, 82,569 (Dec. 28, 2000). I make no findings regarding whether Respondent could have availed itself of this option and exempted certain ePHI from non-disclosure requirements. Suffice it to say that Respondent does not argue it made any effort to do so.

Third, Respondent argues that actions by its employees that it characterizes as "unsanctioned" and by a thief (the person who stole the laptop) cannot be imputed to Respondent and are therefore no basis for liability. Respondent's brief at 44-47. It elaborates on this contention by asserting that the two individuals who lost thumb drives were not acting within the scope of their authorized duties when they lost those items and that the thief who stole the laptop was not an agent or employee of Respondent.

Under HIPAA a principal is liable for the acts of its agents, including its employees, who act within the scope of their duties. 45 C.F.R. § 160.402(c). Respondent attempts to show that the two employees who lost thumb drives were acting outside of the scope of their duties in that they were not following Respondent's policies concerning protection of ePHI when they lost the drives. But, the fact that the employees contravened Respondent's policies doesn't put their actions outside of the scope of their official duties. These employees – both of them – were transporting data for work-related activities. They may have been doing it improperly and in violation of Respondent's policies, but their actions nevertheless were intended to discharge their duties as employees.

Respondent argues that OCR improperly puts the onus for the disclosure of ePHI contained in the stolen laptop on Respondent and the employee who owned the laptop – and who, according to Respondent, did nothing wrong – rather than on the thief who stole the laptop. It characterizes this case as being one in which OCR attempts to blame the victim and not the thief for the wrongful taking of information. However, this case is not in any respect about wrongful taking. This case is about Respondent's failure to *protect* ePHI from disclosure including from theft.

It is easy to lose sight of what is really at issue here in the blizzard of arguments and counterarguments. This case is in its present posture because Respondent recognized a problem, consisting of the vulnerability of its ePHI to unauthorized disclosure including by loss or theft, devised a mechanism to protect ePHI that included encryption of devices, and failed to implement that mechanism. The theft of the laptop illustrates why it was essential for Respondent to implement its encryption policy.

2. Penalty Amounts

OCR requests that I impose civil money penalties against Respondent pursuant to the penalty provisions of 45 C.F.R. Part 160, Subpart D. The regulations in this subpart allow for the impositions of civil money penalties against a covered entity that violates an "administrative simplification provision." 45 C.F.R. § 160.402(a).

Noncompliance with the requirements of 45 C.F.R. § 164.312 and 45 C.F.R. § 164.502 constitutes violations of an administrative simplification provision.

Penalty amounts are determined by criteria set forth at 45 C.F.R. §§ 160.404 and 160.408. The regulations establish four tiers of penalty ranges. These tiers are defined as violations that: (i) the covered entity did not know about and would not have known about by exercising reasonable diligence; (ii) are due to reasonable cause and not due to willful neglect; (iii) are due to willful neglect and are corrected within 30 days of when the covered entity knew or by exercising due diligence would have known about the violations; and (iv) are due to willful neglect and are not corrected within 30 days. 45 C.F.R. § 160.404(b)(2)(i)-(iv).

OCR asserts, and I agree, that the violations in this case meet the "reasonable cause" test of 45 C.F.R. § 160.404(b)(2)(ii). "Reasonable cause" is defined at 45 C.F.R. § 160.401 to mean:

> [A]n act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

Respondent knew that its ePHI was subject to exposure through disclosure, including inadvertent disclosure, through data loss or theft. It was alerted to these risks by the fact that in 2005 a thief stole a laptop containing information of about 4000 of Respondent's patients. OCR Ex. 79. Beginning in 2006 Respondent recognized the vulnerability of its confidential information including ePHI. On numerous occasions thereafter Respondent acknowledged that risk. However, Respondent failed for years to take the action that it had determined to be necessary to address the identified risk – encryption of its mobile data devices – despite its knowledge of the dangers posed by failure to encrypt. As a consequence, the losses of ePHI that Respondent experienced in 2012 and 2013 were foreseeable. Respondent knew or should have known that these losses would be the consequences of its failure to encrypt its devices and would cause the disclosure of confidential information.

Respondent argues that, if any violations occurred, they fell within the first tier of noncompliance. Respondent brief at 48-49. It contends that it neither knew nor could have known that a thief would break into an employee's home and steal a laptop. It asserts that it could not have known that employees would choose to use unencrypted USB drives for storage of confidential information and that these employees would subsequently lose those devices.

I agree that Respondent could not have known in advance about the specific events that caused ePHI to be disclosed in 2012 and 2013. But, that isn't the issue. Respondent had a clear awareness of the *risk* of loss through accidental disclosure. Allowing unencrypted ePHI to be stored on mobile devices exposed that information to the risk of theft or loss, a risk that Respondent knew about, not only by virtue of the 2005 laptop theft, but because it had repeatedly assessed and discussed that risk. The knowledge of that risk is precisely why Respondent ordered in 2008 that all of its mobile devices be encrypted.

Respondent argues that the Secretary concluded that he would not impute culpability to an entity where its agent (an employee) acts consciously in a manner that is adverse to his or her employer, citing 75 Fed. Reg. 40,868, 40,878-40,879 (July 14, 2010). That may be so but Respondent's culpability in this case does not hinge on whether its employees or agents acted in ways that were adverse to Respondent's interests. Respondent's liability – and its culpability – emanates from its failure to address the risk that ePHI could be disclosed via the theft or loss of mobile devices containing such information. As I have discussed, Respondent was well aware of that risk, devised a plan to ameliorate it, and failed to execute on that plan. The failure by Respondent to do what it announced it would do, to encrypt all mobile devices, was the proximate cause of the subsequent ePHI loss.

Respondent seeks to turn the penalty issue on the question of whether its employees played by Respondent's rules governing management of ePHI. For example, it asserts that one of the employees who lost an unencrypted USB drive had been supplied by Respondent with an IronKey encrypted thumb drive but failed to utilize it. However, employee compliance with Respondent's policies is not the substance of OCR's case nor do I find it to be relevant to the issue of Respondent's noncompliance. The question is whether Respondent took the necessary steps to address the risk that it had identified – the potential for data loss due to the storage of ePHI on unencrypted devices. As I have explained, the failure to address that risk is the sum and substance of Respondent's noncompliance. Had it done so, then unauthorized acts by Respondent's employees might be relevant to the issue of compliance. But, failure by Respondent to take the security measures that it had identified as necessary renders irrelevant the issue of whether employees were playing by the rules, because that failure created a risk *whether or not* Respondent's employees did so.

Penalty amounts for second tier violations are bounded as follows: civil money penalties may be assessed in amounts ranging from $1000 up to $50,000 for each violation and may not exceed $1,500,000 for identical violations committed during a calendar year. 45 C.F.R. § 160.404(b)(2)(ii)(A), (B). OCR requests that I impose two penalties falling within the ranges permitted by the second tier: penalties of $2,000 per day for each day of a period that began on March 24, 2011

and that continued through January 25, 2013, in order to remedy Respondent's failure to encrypt ePHI; and penalties of $1,500,000 per year for the years 2012 and 2013 to remedy the loss of ePHI pertaining to about 31,000 individuals in 2012 and more than 3500 individuals in 2013.

OCR argues that each day from March 24, 2011 and continuing through January 25, 2013, constitutes a separate violation by Respondent of the requirement of 45 C.F.R. § 164.312(a) that it develop and implement a mechanism to protect ePHI from unauthorized disclosure.

I find both the duration and amount of these penalties to be reasonable, and I sustain them. The undisputed facts plainly support a finding that Respondent was noncompliant on each day of the period at issue. Respondent was acutely aware of the risks attendant with its failure to protect ePHI. It not only identified those risks, but also concluded that there was a high level of risk if it failed to protect such data. It concluded also that the mechanism that it would use to protect ePHI was to encrypt its mobile devices. But, it failed to do so for years. It is not unreasonable at all to count each day of Respondent's failure to protect its devices as a violation given its assessment of the risk resulting from failure to do so and its inaction in the face of that risk.

The daily penalties that OCR requests that I impose are a small fraction of the maximum allowable daily amount of $50,000 for second tier penalties. I find these amounts to be reasonable given that they are so low but also because the undisputed facts prove the presence of aggravating factors that amply justify the penalty amounts. I find also that the annual penalties that OCR requests that I impose are reasonable, given the level of Respondent's culpability – its failure to implement encryption despite having decided that it would do so and in the face of knowledge of the risks resulting from failure to encrypt – and the number of individuals affected by the unauthorized disclosure of ePHI. As I have discussed, Respondent's noncompliance persisted for years despite the fact that Respondent was well aware of the risks resulting from that noncompliance. 45 C.F.R. § 160.408(a)(2). The unauthorized disclosure of ePHI pertained to more than 33,000 individuals. 45 C.F.R. § 160.408(a)(1).

Respondent argues that, at most, it committed three violations of regulatory requirements, asserting that the only violations constitute the theft of a laptop containing unencrypted ePHI and the loss of two unencrypted thumb drives containing ePHI. Respondent brief at 54-55. I disagree with this analysis. The violations pertaining to failure to protect ePHI from unauthorized disclosure aren't the specific events resulting in data loss. The daily violations are the ongoing failure by Petitioner to protect patient ePHI from unauthorized disclosure, violations that persisted day after day for years. Those violations plainly justify

imposing per-diem penalties during the period when Respondent was non-compliant. 45 C.F.R. § 164.312(a).

However, Respondent also violated regulations in that it disclosed ePHI pertaining to more than 33,000 individuals in incidents occurring in two calendar years, 2012 and 2013. In 2012 Respondent impermissibly disclosed ePHI pertaining to about 30,000 individuals as a result of theft of a laptop and the loss of an unencrypted thumb drive, and in 2013 it impermissibly disclosed ePHI pertaining to more than 3500 individuals due to the loss of an unencrypted thumb drive.

It is reasonable to count the loss of ePHI for each affected individual as a separate violation and to calculate penalties for these violations up to the $1,500,000 annual cap. The regulation allows for a penalty to be imposed for each violation. 45 C.F.R. § 160.404(b). Counting the ePHI loss on a per-capita basis reflects the gravity of the loss. If a violation was limited to the incident in which ePHI was lost (theft or loss of a thumb drive), then a loss of a vast amount of ePHI would count exactly as much as the loss of ePHI pertaining to only one person. That makes no sense.

Respondent argues that the penalties that OCR determined, and that I approve, are arbitrary and capricious. Respondent brief at 55-58. It makes its case for this argument by citing to other instances of ePHI loss and by claiming that remedies imposed for such losses were far more lenient than what OCR requested in this case. However, I do not evaluate penalties based on a comparative standard. There is nothing in the regulations that suggests that I do so. Furthermore, doing so would be impractical because a penalty determination in any given case may rest on a myriad of case-specific facts, many of which are not apparent in the documents that announce the imposition of a remedy. Rather than use comparison, I base my determination on the undisputed facts of this case when measured against the requirements of the regulations. Suffice it to say that I find the penalties proposed by ORI to be reasonable based on the undisputed facts of this case.

Respondent also argues that mitigating factors require reduction of the penalty amounts. Respondent brief at 62-64. It contends that the penalties should be reduced given the absence of facts showing that its violations: caused physical or financial harm; harmed anyone's reputation; or hindered anyone from obtaining health care. It cites also the many steps that it took aside from encrypting its devices in order to protect ePHI.

However, and as I have stated, the penalties that I determine to impose are but a small fraction of the maximum penalties that are permitted by regulation. Penalties of $2000 are only 1/25th of the maximum allowable amount for daily

penalties. The annual penalties of $1,500,000 appear to be large but come to less than $90 for each violation committed by Respondent. The reality is that the penalties imposed in this case are quite modest given the gravity of Respondent's noncompliance.

I note, furthermore, that the penalties are miniscule when compared with Respondent's size and the volume of business that it does. It is a multi-billion dollar per year business. OCR Ex. 82. The sheer size of Respondent's operations and the enormous amount of revenue that it generates, argue against reducing the penalty amounts. Remedies in this case need to be more than a pinprick in order to assure that Respondent and similarly situated entities comply with HIPAA's non-disclosure requirements.

Respondent argues additionally that I should disregard the aggravating factors in this case. Respondent brief at 65-66. It asserts that its failure to encrypt devices should not be considered aggravating inasmuch as applicable regulations do not require that devices be encrypted. This is a rehash of the argument that Respondent makes concerning its liability, reducing to a contention that Respondent should not be held accountable for its failure to encrypt its devices because the regulations don't specifically require that devices be encrypted. I will not re-analyze this issue except to point out that it was Respondent that chose to encrypt its devices to address the high risk that it would lose ePHI. Once it embarked on that course it was obligated to either complete it or replace it with some other mechanism to protect ePHI, neither of which it did. Its persistent failure to carry out encryption left its ePHI naked, exposed to the risk of theft and/or loss. That failure over a period of years is plainly an aggravating factor.

Respondent also contends that it should be granted a waiver from penalties, citing 45 C.F.R. § 160.412, and contending that in this case the penalties are excessive relative to the violations cited by OCR. I do not find any basis for a waiver. As I have discussed, the penalties in this case are reasonable given the gravity of Respondent's noncompliance and the number of individuals potentially affected. What is most striking about this case is that Respondent knew for more than five years that its patients' ePHI was vulnerable to loss and theft and yet, it consistently failed to implement the very measures that it had identified as being necessary to protect that information. Respondent's dilatory conduct is shocking given the high risk to its patients resulting from unauthorized disclosure of ePHI, a risk that Respondent not only recognized but that it restated many times.

Steven T. Kessel
Administrative Law Judge